

Scansione con il firewall windows disabilitato:

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sV 192.168.50.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:37 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 13:38 (0:00:32 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 13:39 (0:01:05 remaining)
Nmap scan report for 192.168.50.120
Host is up (0.0033s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: SABRINA-PC; OS: Windows; CPE: o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.68 seconds
```

Scansione con il firewall abilitato:

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.120 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 13:44 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 23.00% done; ETC: 13:48 (0:02:37 remaining)
Stats: 0:02:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 68.50% done; ETC: 13:48 (0:01:03 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 87.00% done; ETC: 13:48 (0:00:26 remaining)
Stats: 0:03:10 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 94.50% done; ETC: 13:48 (0:00:11 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 96.50% done; ETC: 13:48 (0:00:07 remaining)
Nmap scan report for 192.168.50.120
Host is up.
All 1000 scanned ports on 192.168.50.120 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.65 seconds
```

## Facoltativo

### Log del firewall

```
pfirewall - Blocco note
File Modifica Formato Visualizza ?
#Version: 1.5
#Software: Microsoft windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tpack tc

2024-09-17 20:06:57 DROP TCP 192.168.50.100 192.168.50.120 57142 445 60 S 3615614056 0 32120 - -
2024-09-17 20:06:58 ALLOW UDP fe80::54b6:eec4:2272:1afe ff02::1:2 546 547 0 - - - - - SEND
2024-09-17 20:06:59 DROP TCP 192.168.50.100 192.168.50.120 57144 445 60 S 336434330 0 32120 - -
2024-09-17 20:06:59 DROP TCP 192.168.50.100 192.168.50.120 42522 135 60 S 3183522409 0 32120 - -
2024-09-17 20:07:02 DROP TCP 192.168.50.100 192.168.50.120 36414 139 60 S 3358372722 0 32120 - -
2024-09-17 20:07:03 DROP TCP 192.168.50.100 192.168.50.120 36416 139 60 S 2474210327 0 32120 - -
2024-09-17 20:07:04 DROP TCP 192.168.50.100 192.168.50.120 50150 49153 60 S 849174482 0 32120 - -
2024-09-17 20:07:05 DROP TCP 192.168.50.100 192.168.50.120 50158 49153 60 S 4184521018 0 32120 - -
2024-09-17 20:07:06 DROP TCP 192.168.50.100 192.168.50.120 53528 49156 60 S 1303168121 0 32120 - -
2024-09-17 20:07:06 DROP TCP 192.168.50.100 192.168.50.120 46650 5357 60 S 1244835412 0 32120 - -
2024-09-17 20:07:07 DROP TCP 192.168.50.100 192.168.50.120 53536 49156 60 S 1200053929 0 32120 - -
```

```
pfirewall - Blocco note
File Modifica Formato Visualizza ?
wall
l src-ip dst-ip src-port dst-port size tcpflags tcpsyn tpack tcpwin icmp type icmpcode info path

168.50.100 192.168.50.120 57142 445 60 S 3615614056 0 32120 - - - RECEIVE
0::54b6:eec4:2272:1afe ff02::1:2 546 547 0 - - - - - SEND
168.50.100 192.168.50.120 57144 445 60 S 336434330 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 42522 135 60 S 3183522409 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 36414 139 60 S 3358372722 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 36416 139 60 S 2474210327 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 50150 49153 60 S 849174482 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 50158 49153 60 S 4184521018 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 53528 49156 60 S 1303168121 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 46650 5357 60 S 1244835412 0 32120 - - - RECEIVE
168.50.100 192.168.50.120 53536 49156 60 S 1200053929 0 32120 - - - RECEIVE
```

Il log è strutturato in colonne con le seguenti informazioni:

- **src-ip**: Indirizzo IP sorgente.
- **dst-ip**: Indirizzo IP di destinazione.
- **src-port**: Porta sorgente.
- **dst-port**: Porta di destinazione.
- **size**: Dimensione del pacchetto.
- **tcpflags**: Flag TCP (S per SYN).
- **tcpsyn**: Numero di sequenza SYN.
- **tpack**: Numero di sequenza ACK.
- **tcpwin**: Dimensione della finestra TCP.
- **icmp type** e **icmpcode**: Tipo e codice ICMP (non usati qui).
- **info**: Informazioni aggiuntive (RECEIVE/SEND).
- **path**: Percorso del pacchetto (non popolato in questo esempio).

Questi log forniscono dettagli su pacchetti TCP inviati e ricevuti, specificando la direzione, la sorgente, la destinazione e altri parametri relativi alla comunicazione di rete.

### **Cosa si riesce a trovare?**

Monitorando questi log durante le operazioni di rete, puoi trovare informazioni come:

- **Conferme di connessione e disconnessione di rete:**
  - Eventi che registrano quando una connessione è stata stabilita o terminata, inclusi i dettagli su sorgente, destinazione, porte utilizzate, e protocolli.
- **Modifiche al firewall:**
  - Se vengono aggiunte, rimosse o modificate regole del firewall, queste azioni verranno registrate. È utile per tracciare se un'operazione ha cambiato il comportamento del firewall in modo non previsto.
- **Rilevamento di attacchi o tentativi di accesso non autorizzato:**
  - Se il firewall blocca delle connessioni non autorizzate o se ci sono tentativi di attacco, come scansioni di porte, questi eventi saranno visibili nel log del firewall o nel registro di sicurezza.
- **Trasmissioni o ricezioni di pacchetti inusuali:**
  - Eventi di sicurezza che potrebbero mostrare comportamenti sospetti, come pacchetti TCP non previsti o configurazioni IP inusuali.
- **Errori di connessione o servizi di rete falliti:**
  - Log relativi a problemi di connessione, come errori DHCP, DNS, o TCP/IP. Possono essere utili per risolvere problemi legati a configurazioni di rete o malfunzionamenti.
- **Autorizzazioni e tentativi di accesso:**
  - Se sono abilitati eventi di auditing legati all'accesso alla rete o alle modifiche di configurazione, potresti trovare tracce di chi ha effettuato certe operazioni, quando e da quale macchina.